Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	ET Docket No. 04-295
Communications Assistance for Law Enforcement	)	RM-10865
Act and Broadband Access and Services	)	
	)	

Comments of the American Civil Liberties Union on the Notice of Proposed Rulemaking

Christopher R. Calabrese, Counsel
Barry Steinhardt, Director
American Civil Liberties Union
Technology & Liberty Program
125 Broad Street
17th Floor
New York, NY 10004

Laura W. Murphy, Director
Marvin Johnson, Legislative Counsel
American Civil Liberties Union
Washington Legislative Office
915 15th Street, NW
Washington, DC 20005

November 8, 2004

The American Civil Liberties Union opposes the Notice of Proposed Rulemaking applying the Communications Assistance for Law Enforcement Act (CALEA) to broadband Internet service and Voice over Internet Protocols (VoIP) because it raises significant constitutional, statutory and practical problems and offers no demonstrated security benefit.

The Commission seeks comment on its initial determination that broadband access providers and VoIP providers are subject to CALEA under the substantial replacement provision of the definition of a telecommunications carrier.[1] Specifically the Commission makes two holdings on the basis of the substantial replacement theory:

> [W]e tentatively conclude that facilities-based providers of any type of broadband Internet access, including but not limited to wireline, cable modem, satellite, wireless, and broadband access via the powerline, whether provided on a wholesale or retail basis, are subject to CALEA (with possible limited exception discussed below), because they provide replacement for a substantial portion of the local telephone exchange service used for dial-up Internet access service and such treatment is in the public interest. (citations omitted)[2]

and

> We tentatively conclude that providers of managed VoIP services, which are offered to the general public as a means of communicating with any telephone subscriber, including parties reachable only through the PSTN, are subject to CALEA. We believe that such VoIP service providers satisfy each of the three prongs of the Substantial Replacement Provision with respect to their VoIP services. That is, they provide an electronic communication switching or transmission service that replaces a substantial portion of local exchange service for their customers in a manner functionally the same as POTS service; and the public interest factors we consider at a minimum – *i.e.*, the effect on competition, the development and provision of new technologies and services, and public safety and national security – support subjecting these providers to CALEA. (citations omitted)[3]

We believe that the Commission's application of CALEA both to broadband and to VoIP is an improper reading of the statutory language and contrary to Congressional intent. Comments by the Center for Democracy and Technology (CDT) and other commentators will address this statutory argument in detail. We endorse CDT's comments in regards to the proper statutory interpretation of CALEA and Congressional intent, and will simply state that both the definition of telecommunications carriers and section 1002(b) clearly exempt information services from CALEA's requirements. We believe that both the definition of information services and Congressional intent make clear that both broadband and VoIP are information services and hence exempt from CALEA.[4]

---

[1] The definition of telecommunications carriers includes "a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter." 47 U.S.C. §1001(8).

[2] At paragraph 47.

[3] At paragraph 56.

[4] 47 U.S.C.A §1002(b); 47 U.S.C.A. § 1001(6) (The term "information service" means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and includes a service that permits a customer to retrieve

Because the majority of the Commission's notice is aimed at examining the impact of CALEA on VoIP, we will direct the rest of our comments to this subject. Specifically we address the following issues:

- What is "call identifying information" in the Internet context?
- Does application of CALEA to VoIP meet the public interest prong of the substantial replacement test?
- Who should bear the cost of wiretap orders?
- Is it permissible for a telecommunications carrier to contract out its surveillance obligations to a 3rd party?

We will treat all of these questions in turn. Of special note is the next section – the question of call identifying information in an Internet context. If this issue is not addressed, significant portions of the proposed regulatory structure may be constitutionally infirm and hence invalid.

Constitutional Issues in Applying Call Identifying Information in an Internet Context

The Commission requested comment on whether it needs to clarify the term "call identifying information" for VoIP services. We believe that this definition requires significant clarification in order avoid potential constitutional problems.

In *Berger v. New York*, the Supreme Court ruled that subjects of electronic surveillance were protected by the Fourth Amendment's restrictions against unreasonable searches and seizures.[5] The Court held in *Berger* that lengthy, continuous or indiscriminate electronic surveillance violated the Fourth Amendment.[6] A subsequent ruling, *Katz v. United States* held that surveillance must be approved by a magistrate and must be "limited, both in scope and duration, to the specific purpose of establishing the contents of the petitioner's unlawful telephonic communications."[7] These holdings provide the underpinnings for both Title III and CALEA.

As the Commission is aware the content of phone conversations is subject to the exacting strictures of the 4th Amendment as embodied by *Berger*, *Katz* and Title III. On the other hand, because it is provided willingly to phone companies, call identification information is not subject to the 4th Amendment and the standard of proof is much lower.[8] This distinction is important for VoIP because these technologies use digital

---

stored information from, or file information for storage in, information storage facilities); House Report, at 18.

[5] *Berger v. New York*, 388 U.S. 41.

[6] *Id.*

[7] *Katz v. United States,* 389 U.S. 347, 354.

[8] 18 U.S.C. 3122(b)(2) (the information is likely to be obtained is relevant to an ongoing criminal investigation).

packet networks. *U.S. Telecom v. FCC* is the most current precedent on this issue.[9] As the court explains in *U.S. Telecom*:

> In digital packet-switched networks, communications do not travel along a single path. Instead, a call is broken into a number of discrete digital data packets, each traveling independently through the network along different routes. Data packets are then reassembled in the proper sequence at the call's destination. Like an envelope, each digital packet has two components: it contains a portion of the communication message, and it bears an address to ensure that it finds its way to the correct destination and is reassembled in proper sequence.[10]

The court acknowledged that the fact that each packet contained both types of information raised potential privacy concerns. It deferred to an ongoing effort by the Commission, working through industry, to address those concerns. However, in the four years since *U.S. Telecom* was decided no single unified standard for identifying and culling call identification information has developed. Instead the industry and law enforcement have proceeded in an ad hoc manner that treats different packet mode services in different manners and too often results in the law enforcement gaining access to the entire packet or packet stream, and then culling the information it desires.

This makeshift process must end. The Commission must recognize that packet based communications, especially those that utilize the Internet, are fundamentally different than previous communications technologies, and that their call identification information is different as well. The Commission must review the architecture of different packets and determine what identifying information is common to each and can be extracted without law enforcement viewing or holding call content information. Balancing law enforcement interests and the "privacy and security of communications and call-identifying information not authorized to be intercepted"[11] is a core tenent of CALEA.

More importantly, protecting the content of an individual's call is a requirement under the 4th Amendment. As the court stated in *U.S. Telecom*:

> [N]othing in the Commission's treatment of packet-mode data requires carriers to turn over call content to law enforcement agencies absent lawful authorization. Although the Commission appears to have interpreted the J-Standard as expanding the authority of law enforcement agencies to obtain the contents of communications, the Commission was simply mistaken. All of CALEA's required capabilities are expressly premised on the condition that any information will be obtained "pursuant to a court order or other lawful authorization." CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing

[9] *U.S. Telecom v. FCC,* 227 F.3d 450.
[10] *U.S. Telecom* at 464.
[11] 47 U.S.C. §1002(a)(4)(A).

> legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is "not authorized to be intercepted."[12]

The Commission's responsibility to safeguard both call identifying and call content information is clear.

The difficulty in isolating call identifying information also raises a second constitutional problem – the danger that law enforcement will gain access to unauthorized communications as part of an order authorizing them to secure the content of calls. Currently law enforcement and service providers face significant technological hurdles in linking a particular packet to the individual communication whose interception has been authorized. As the International Engineering Consortium notes:

> Another influential element in the ongoing Internet-telephony evolution is the VoIP gateway. As these gateways evolve from PC–based platforms to robust embedded systems, each will be able to handle hundreds of simultaneous calls. Consequently, corporations will deploy large numbers of them in an effort to reduce the expenses associated with high-volume voice, fax, and videoconferencing traffic. The economics of placing all traffic— data, voice, and video—over an IP–based network will pull companies in this direction, simply because IP will act as a unifying agent, regardless of the underlying architecture (i.e., leased lines, frame relay, or ATM) of an organization's network.[13]

This technical reality means that an increasing number of communications, both of different types and by different individuals, will be difficult to distinguish at the packet level. It is not a constitutionally permissible outcome to simply give law enforcement access to an entire data stream and allow them to sort out the information that they are lawfully allowed to see. This type of surveillance is both indiscriminate and almost unlimited in violation of the constitutional strictures created by *Berger* and *Katz* and by the language of Title III.

Public Interest Prong of the Substantial Replacement Provision

The Commission has asked for comment on whether application of CALEA to VoIP meets the third prong of the substantial replacement test, namely "is it in the public interest to deem such a person or entity to be a telecommunications carrier for the purposes of this title."[14] The Commission states three factors that should be considered in making this determination: whether it would promote competition; whether it would encourage the development of new technologies; and whether it would protect public

---

[12] *U.S. Telecom* at 465.
[13] International Engineering Consortium**,** *Voice over Internet Protocol,* 2003.
[14] 47 U.S.C. §1001(8)(B)(ii).

safety.[15] The application of the substantial replacement test in this context badly fails all three of these tests.

CALEA harms competition by imposing an unnecessarily high regulatory burden on the industry. The Public Switching Telephone Network (PSTN) is a large, well-established network whose technology only changes gradually over time and is dominated by a few large players. VoIP and the Internet is a new, fast moving network, subject to rapid technological change and inhabited by a wide variety of small, medium and large companies. Many of the rules from this older industry simply do not, and should not, apply to this new technology. The cost of CALEA compliance will almost certainly drive some of these small and medium sized companies either out of the market or out of business all together. In fact some of these companies offer their services for free and hence their operating margins and ability to absorb new regulatory costs is exceedingly low. A reduction in the number of companies offering VoIP represents a direct harm to competition.

These high regulatory costs will hinder competition in other ways as well. They will represent a high barrier to entry, limiting other entities from entering the market and competing with existing actors. As we will discuss below, they will also hinder the development of new technology. This will disproportionately impact smaller companies that rely on rapid technological advances to stay ahead of their larger, better capitalized competitors. In short, imposition of CALEA on VoIP will rob this vibrant market of many of the competitive factors that make it so promising and force it to conform to the model of the old PSTN.

Imposing CALEA on VoIP will also stifle the development of new technology. As we described above it will drive potential innovators out of the market, limiting the overall base for new innovation. It will likely force companies to replicate unnecessary features of the old PSTN. While neither law enforcement nor the Commission has specified what call identifying information it will expect companies to provide, past history suggests that, at minimum, this information will consist of the items described on the FBI "punch list."[16] Hence, instead of working to determine what new features customers might want which are possible as part of an Internet based phone application, providers will be forced to recreate old models from the PSTN which are both unnecessary, costly and grant them no competitive advantage over their PSTN rivals.

---

[15] At paragraph 45.

[16] As the Commission noted in footnote 26 of the NPRM, the six FBI "punch list" requirements are: "dialed digit extraction," which would provide to LEAs those digits dialed by a subject after the initial call setup is completed; "party hold/join/drop," which would provide to LEAs information to identify the active parties to a conference call; "subject-initiated dialing and signaling," which would provide to LEAs access to all dialing and signaling information available from the subject, such as the use of flash-hook and other feature keys; "in-band and out-of-band signaling," which would provide to LEAs information about tones or other network signals and messages that a subject's service sends to the subject or associate, such as notification that a line is ringing or busy; "subject-initiated conference calls," which would provide to LEAs the content of conference calls supported by the subject's service; and "timing information," which would provide to LEAs information necessary to correlate call-identifying information with call content. (citations omitted)

Further, the Commission proposed rulemaking would do little or nothing to promote public safety. In fact it is likely to actually make the public less safe and endanger the privacy of every American. Building in a "back-door" to provide easy access for law enforcement also creates a loophole that can be exploited by hackers, criminals and terrorists. While the distributed nature of Internet communications currently provides a powerful natural barrier to effective surveillance on specific individuals, adoption of CALEA will force the creation of exactly this type of vulnerability. Criminals will simply have to penetrate the security surrounding the surveillance system itself because the provider, at the behest of law enforcement, will already have solved the vastly more difficult technical problem of isolating specific communications. This type of security attack will not only create a massive invasion of privacy it will enable a host of other crimes that rely on securing personal information such as identity theft and fraud. Perhaps worst of all, because the law enforcement has not provided a single instance when it was unable to execute a lawful wiretap order, this damage to our nation's security will not be counterbalanced with any demonstrated security benefit.

Ultimately all of the burdens created by applying CALEA to VoIP means the Commission's rulemaking is likely to violate another provision of CALEA, section 107.[17] This section states that in exercising its authority to set technical standards for CALEA, the Commission must "serve the policy of the United States to encourage the provision of new technologies and services to the public."[18] The Commission's current policy will result in a much different result than that intended by the statute – the crippling or destruction of an entire industry. Because the Internet is global in scope, VoIP is a mobile industry that does not have to be based in the United States and can locate anywhere. The U.S. is currently a leader in the VoIP because of our strong technology base, flexible regulatory structure and role as a historical center for telecommunications. However, if the U.S. chooses to pass new regulations that impose high costs and stifle innovation, it is almost certain that either the nascent VoIP industry in the United State will be forced to relocate or it will be overtaken by other, foreign competitors that do not face the same cumbersome regulatory hurdles and hence can offer a lower cost service.

The Commission's Chairman, Michael Powell, has characterized VoIP as, "probably the most significant paradigm shift in the entire history of modern communications, since the invention of the telephone."[19] As it matures, this industry is almost certain to grow, providing the high technology, high wage jobs upon which the U.S. economy depends. The Commission must decide whether it was to ruin a new American industry for an illusory security benefit that will vanish once the VoIP industry is forced to relocate overseas.

The Cost of Wiretap Orders

[17] 47 U.S.C. §1006.
[18] *Id.*
[19] *FCC chief plans no Internet telephony regulation*, REUTERS, Jan. 22, 2004.

The Commission has asked for comment on who should bear the cost of CALEA implementation costs and has tentatively concluded that it should be telecommunications carriers and ultimately consumers. We oppose this determination.

Instead the Commission should be guided by the provisions of Section 107 of the Act.[20] This section describes the criteria by which the Commission should abide in setting technical standards for compliance with CALEA. Specifically, technical standards shall:

> **(1)** meet the assistance capability requirements of section 1002 of this title by cost-effective methods;
> **(2)** protect the privacy and security of communications not authorized to be intercepted;
> **(3)** minimize the cost of such compliance on residential ratepayers;
> **(4)** serve the policy of the United States to encourage the provision of new technologies and services to the public; and
> **(5)** provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 1002 of this title during any transition period.[21]

As subsection (3) states explicitly, and subsections (1), (2), and (4) implicitly, the chief concern of the Commission must be setting the least expensive costs possible with the end goal of minimizing expenses to the consumer. Nothing in these standards describes granting law enforcement the best access to communications or even mention law enforcement access at all.

If the Commission persists in this rulemaking, it must be governed by Congress's clear and unequivocal intent as expressed in the statute: minimize cost, especially for the consumer. The Commission's tentative decision completely contravenes this intent. Instead it creates a model where law enforcement, the entity driving all of the costs of the system, bares none of the costs of building the system. This system actually *maximizes* consumer costs because it assures that law enforcement will have every incentive to describe standards that shift the costs of its surveillance from itself to carriers. Carriers in a competitive marketplace will have no choice but to pass these costs along to consumers either directly or indirectly.

Trusted 3rd Parties

The Commission has also asked for comment on the use of trusted 3rd parties to fulfill a telecommunications provider's CALEA requirements. Under the Commission's formulation such a 3rd party would be "a service bureau with a system that has access to a

[20] 47 U.S.C. §1006.
[21] *Id.*

carrier's network and remotely manages the intercept process for the carrier."[22] We find this approach very troubling.

As we have noted previously, one of CALEA's four purposes is "to protect the privacy and security of communications not authorized to be intercepted."[23] Further, any standards the Commission implements under the Act should "protect the privacy and security of communications not authorized to be intercepted."[24] The idea of allowing a trusted 3rd party to manage a company's surveillance directly contravenes these requirements because it has a dramatic, negative impact on the security of information traveling on the Internet and privacy of individuals engaging in those communications.

A trusted 3rd party harms security in at least three ways. The first is that it multiplies the number of entities that can access this sensitive information and hence exposes the entire system to increased vulnerability. Because security systems are only as strong as their weakest point, if the security of a trusted 3rd party is not, in every way, as strong as the security of the telecommunications carrier and law enforcement, then security has been compromised. In addition, the number of people with access to sensitive communications increases, expanding the possibility for abuse from insiders.

The second threat to security is that trusted 3rd parties would be very attractive targets to criminals and terrorists. If a criminal penetrates the security of a trusted 3rd party he has access to a vast array of communications – all of the communications of a carrier and likely the communications of multiple carriers. Better still from a criminal point of view these communications would already be structured for easy identification and transfer. This is a dream for any terrorist, hacker or spy.

In addition, it is axiomatic that information is vulnerable when it is being transferred. It is outside of a carrier's security system and not yet protected by law enforcement. The use of trusted third parties, especially one that relies on what the Commission describes as an external system approach, makes that vulnerability infinitely worse. Not only does it insert an additional link in the chain of information transfer, it requires *all* communication to be transferred outside of a carrier's security system. Instead of simply transferring a very limited amount of call identifying and call content information in response to a law enforcement request, a carrier would be exposing every communication in its system to vulnerability.

Finally, the idea that these trusted third parties could be owned by law enforcement merits special comment.[25] We believe that this idea would be unconstitutional. Individuals working for a trusted 3rd party would be either government employees or, at minimum, agents of the government. Allowing them to receive and process all communications from a provider would amount to turning over all communications to law enforcement without probable cause of a crime, a lawful warrant

[22] At paragraph 69.
[23] 47 U.S.C. §1002(a)(4)(A).
[24] 47 U.S.C §1006(b)(2).
[25] This possibility was raised in paragraph 75.

or a demonstration of the purpose of the wiretap. In short, this action would be in complete violation of established 4th Amendment law and Title III.

Conclusion

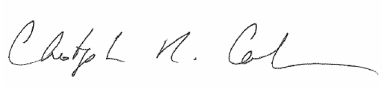
Ultimately the issue of applying CALEA to broadband and VoIP should be left to Congress. By applying the substantial replacement theory in such an indiscriminate manner, the Commission is essentially re-writing CALEA. This type of agency usurpation of Congress's role as the sole federal lawmaker comes with significant cost. Agency overreaching, no matter how well meaning or important its public policy objectives, robs the citizenry of its most significant right – to make, through its duly elected representatives, policy choices that will guide America's future. The role of law enforcement in Internet communications has implications for both the war on terror and free speech. Seeking a balance between security and freedom is the most important ongoing conversation in American life. It deserves to be argued in the halls of Congress.

By so dramatically twisting the statutory language and Congressional intent, the Commissions decision will also cause a host of practical problems. First, it will sow confusion. It will almost certainly face a court challenge, one that would likely last for years and be exacerbated by the need to resolve not only complex statutory issues but also the difficult constitutional issues we raise above. Instead of expanding their service options and customer base, VoIP providers and equipment manufacturers would face uncertainty over the standards for their emerging business and waste resources on costly litigation. Further, as we noted above, this rulemaking requires the balancing of a number of concerns including police surveillance, technological innovation, free speech and economic development. These issues extend far beyond the scope of the Commission's expertise. If this process goes forward it is almost certain to result solution that is less well informed or comprehensive that it would be if undertaken by Congress.

For all of the above stated reasons we believe that the Commission should abandon its tentative conclusion that broadband providers and VoIP providers are telecommunications carriers under CALEA. We further believe that even if the Commission does not withdraw this conclusion, it must comprehensively revisit the definition of call identifying information in an Internet context, bar the use of trusted 3rd parties in implementing CALEA, and force law enforcement to bare the capital costs for new CALEA standards.

Respectfully submitted,

American Civil Liberties Union



By

Christopher R. Calabrese
Barry Steinhardt
Laura W. Murphy
Marvin Johnson